

Student: Yengkong Sayaovong Email: ysayaovo@asu.edu

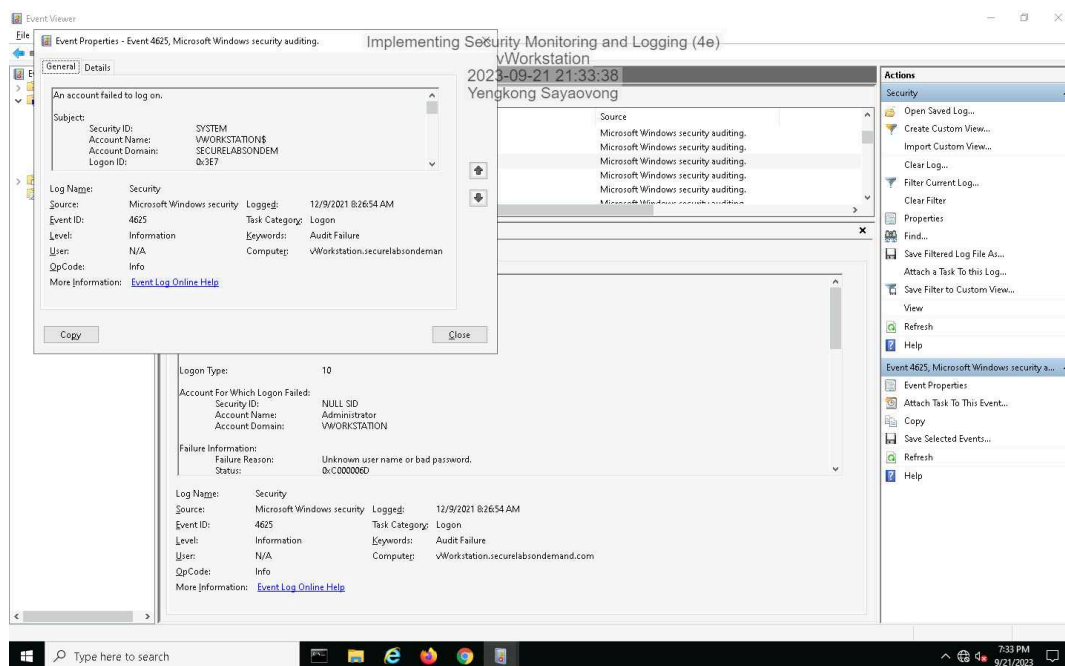
Time on Task: 0 hours, 46 minutes Progress: 91%

Report Generated: Thursday, September 21, 2023 at 11:14 PM

Section 1: Hands-On Demonstration

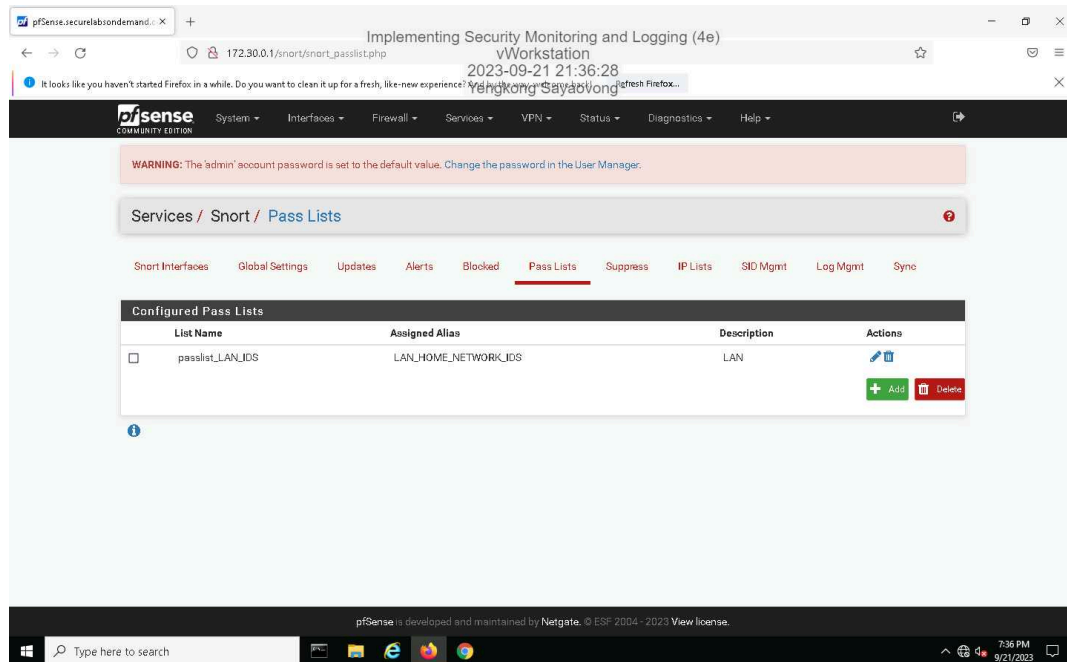
Part 1: Identify Failed Logon Attempts on Windows Systems

8. Make a screen capture showing the **Security Event Properties** dialog box on the **vWorkstation**.

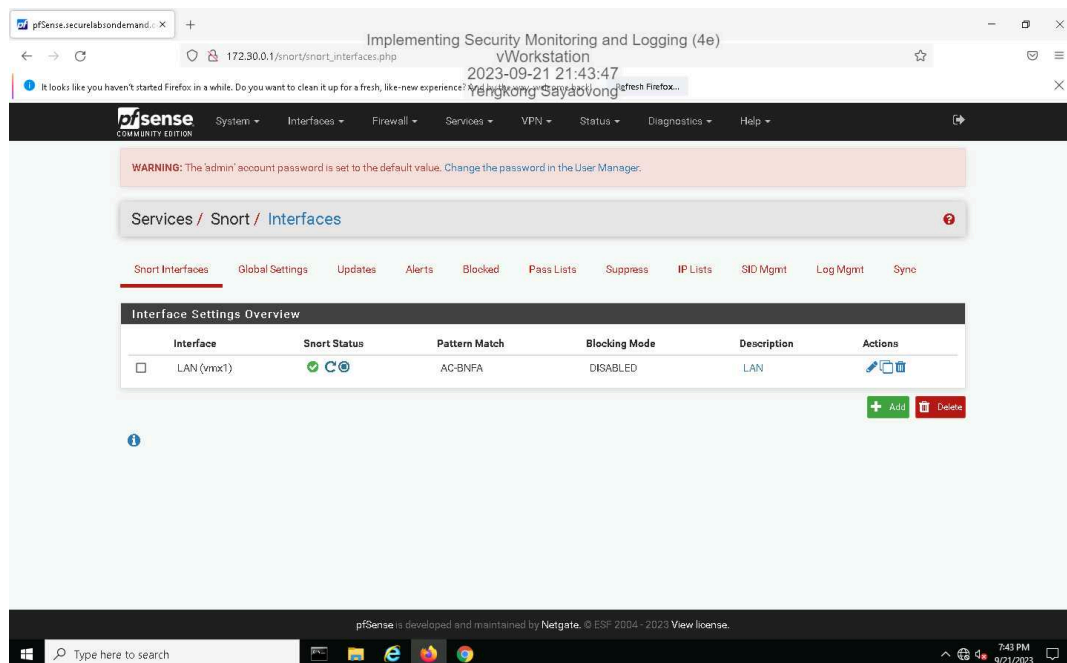


Part 2: Monitor Network Activity with Snort

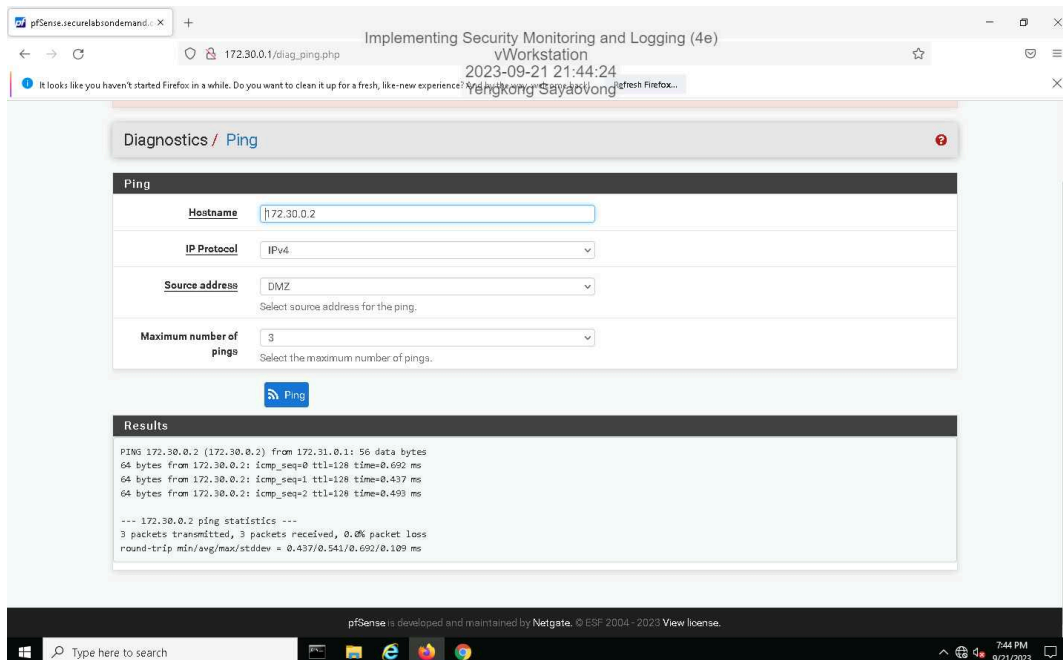
17. Make a screen capture showing the updated Pass Lists page.



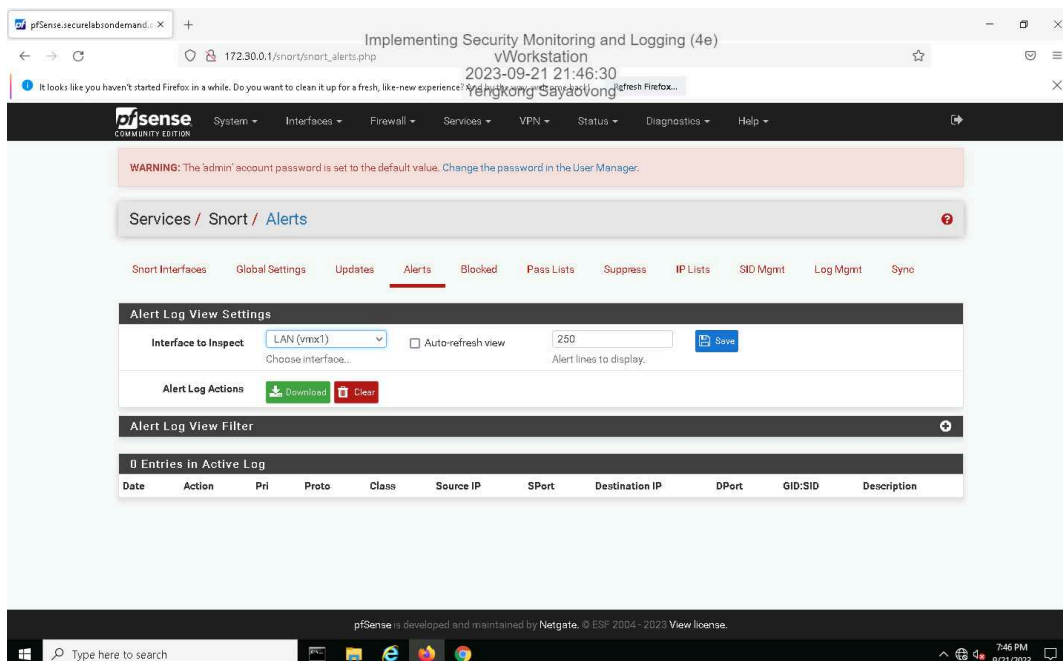
31. Make a screen capture showing the active Snort status on the LAN interface.



36. Make a screen capture showing the successful ping results.



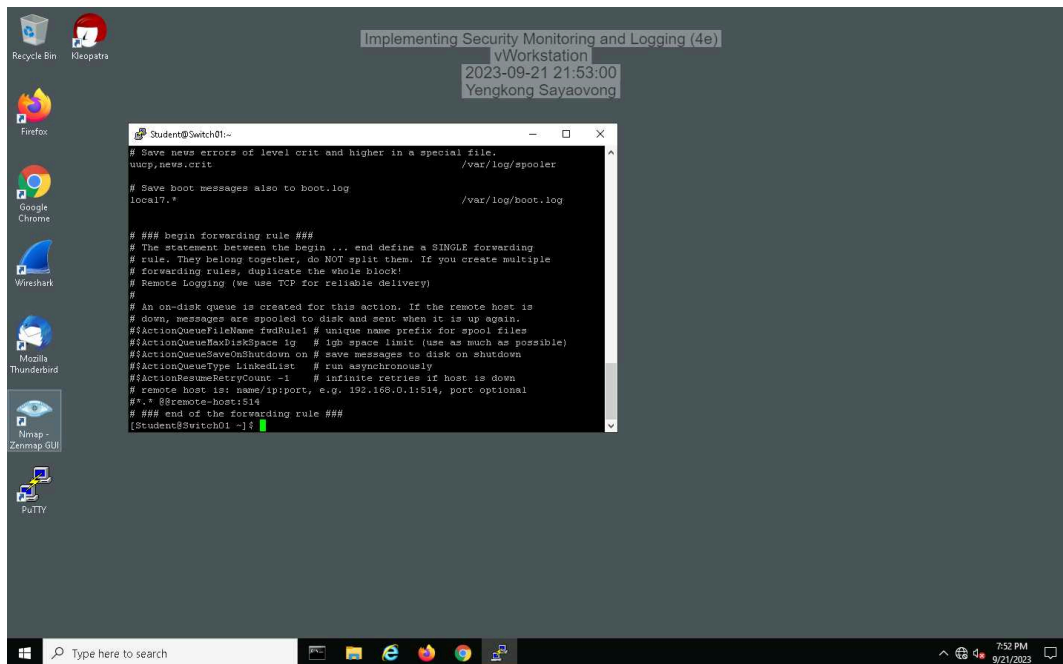
41. Make a screen capture showing the ICMP alerts in the Snort Active Log.



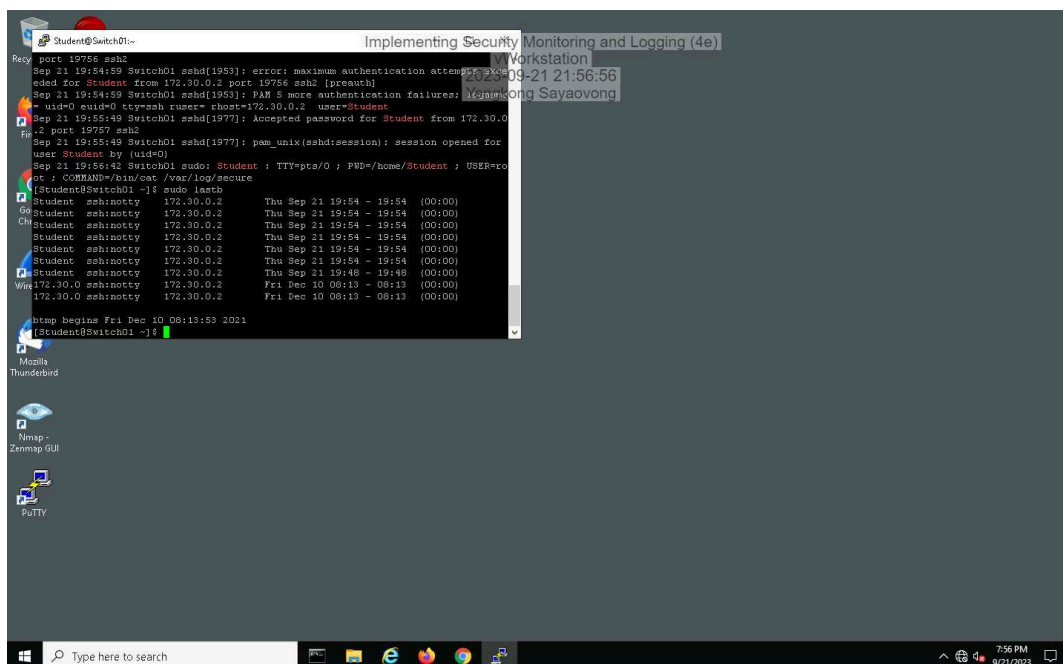
Section 2: Applied Learning

Part 1: Identify Failed Logon Attempts on Linux Systems

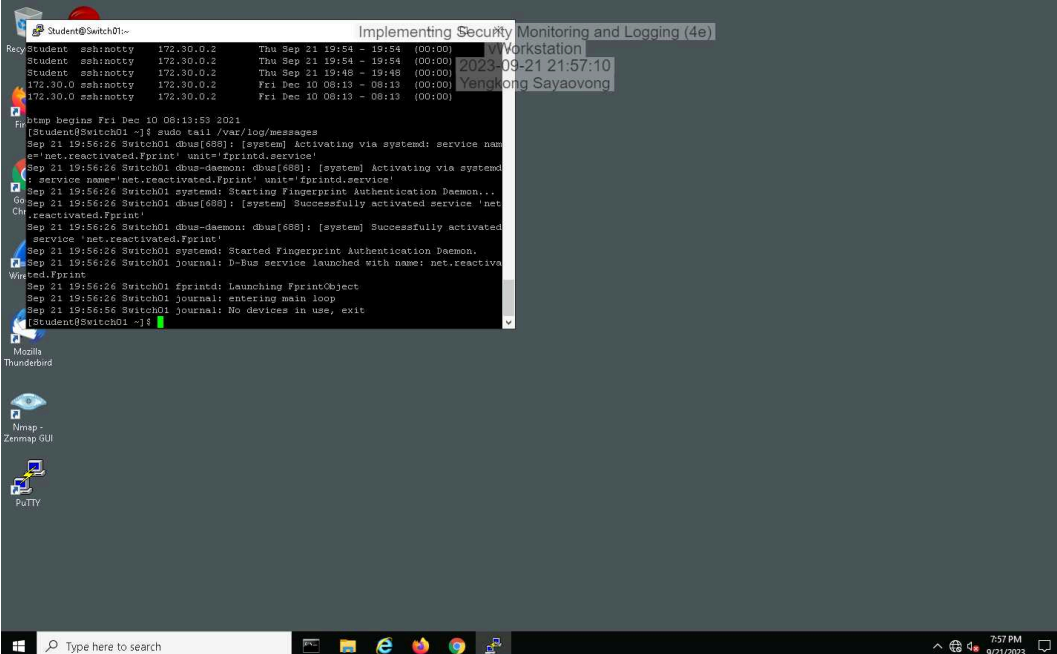
10. Make a screen capture showing the edited `rsyslog.conf` file.



20. Make a screen capture showing the failed login attempts.



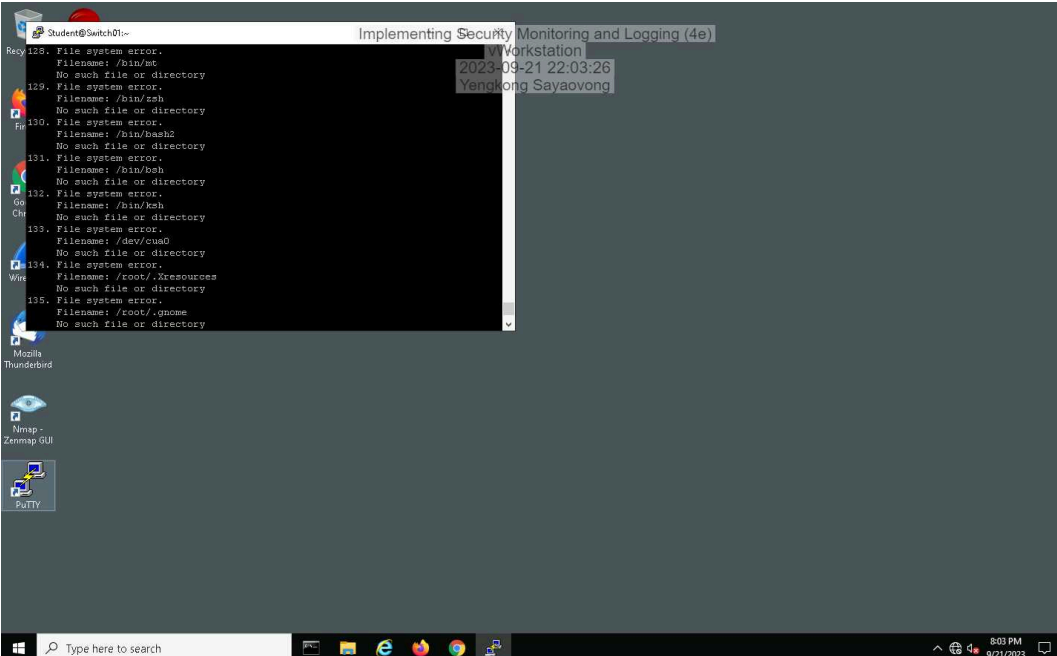
22. Make a screen capture showing the last 10 log messages.



```
Student@Switch01:~$ sudo tail -n 10 /var/log/messages
Sep 21 19:56:26 Switch01 dbus-daemon[688]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service'
Sep 21 19:56:26 Switch01 dbus-daemon[688]: [system] Successfully activated service 'net.reactivated.Fprint'
Sep 21 19:56:26 Switch01 systemd: Starting Fingerprint Authentication Daemon...
Sep 21 19:56:26 Switch01 journal: D-Bus service launched with name: net.reactivated.Fprint
Sep 21 19:56:26 Switch01 fprintd: Launching FprintObject
Sep 21 19:56:26 Switch01 journal: entering main loop
Sep 21 19:56:26 Switch01 journal: NO devices in use, exit
Student@Switch01 ~$
```

Part 2: Monitor File Integrity with Tripwire

12. Make a screen capture showing the Object Summary section for the Tripwire report.

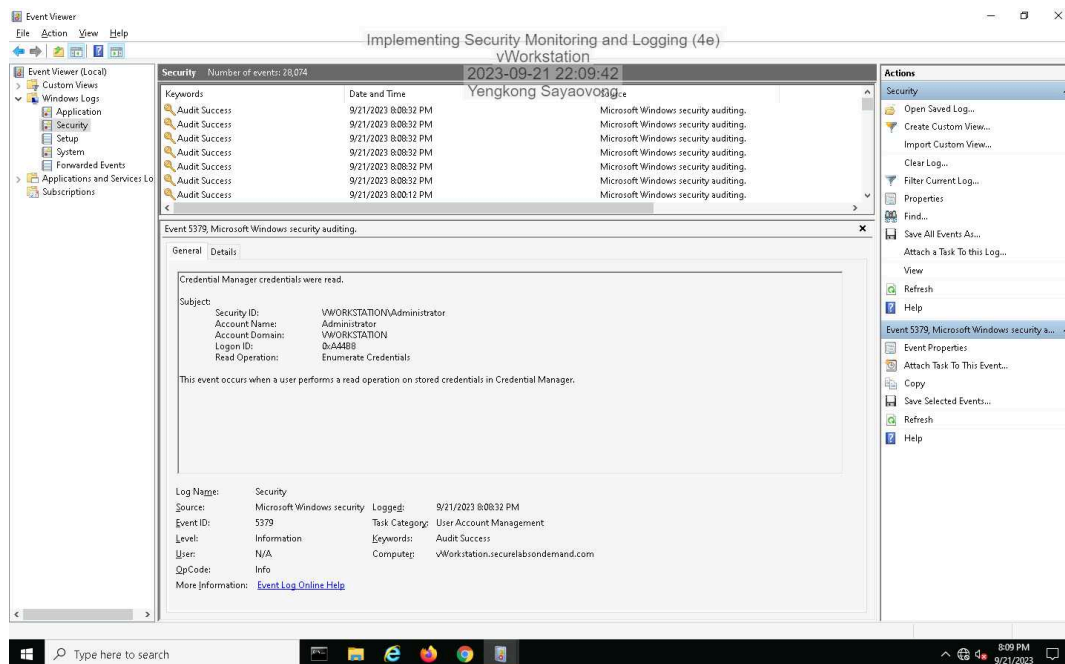


```
128. File system error.
Filename: /bin/ls
No such file or directory
129. File system error.
Filename: /bin/ls
No such file or directory
130. File system error.
Filename: /bin/ls
No such file or directory
131. File system error.
Filename: /bin/ls
No such file or directory
132. File system error.
Filename: /bin/ls
No such file or directory
133. File system error.
Filename: /bin/ls
No such file or directory
134. File system error.
Filename: /bin/ls
No such file or directory
135. File system error.
Filename: /bin/ls
No such file or directory
```

Section 3: Challenge and Analysis

Part 1: Identify Additional Event Types in the Event Viewer

Make a screen capture showing the **Security Event Properties** dialog box for an **Audit Failure** associated with **Event ID 5061**.



Provide a brief explanation of the operation that would generate a security event with Event ID 5061.

Event ID 5061 is the Windows Security Event log entry generated when a Windows Firewall rule is changed. This event is triggered whenever a user or application modifies or creates a new Windows Firewall rule, including changes in scope, protocol, port, program, or other rule settings.

Part 2: Configure Snort as an Intrusion Prevention System

Make a screen capture showing the **Legacy Blocking Mode** enabled on the LAN interface.

Incomplete